



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

09/707,285

11/01/2000

Michael Brownlie

0500.0008210

8456

7590

01/27/2005

Christopher J. Reckamp  
Vedder Price Kaufman & Kammholz  
222 North LaSalle Street,  
Suite 2600  
Chicago,, IL 60601

EXAMINER

DADA, BEEMNET W

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/707,285

Applicant(s)

BROWNLIE ET AL.

Examiner

Beemnet W Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 August 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

1. This office action is in reply to an amendment filed on August 12, 2004. Claims 1-40 are pending.

### ***Response to Arguments***

2. The obviousness type double patenting rejection to claims 1-8 and 10-38 has been withdrawn in view of the Terminal Disclaimer filed on August 12, 2004.

3. Applicant's arguments, filed on August 12, 2004, with respect to the rejection(s) of claim(s) 1-40 under 35 USC 103 (a) over Matyas US Patent 5,164,988 in view of Barlow US Patent 5,204,961 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-40 are rejected under, 35 U.S.C. 103(a) as being unpatentable over Matyas et al, US Patent 5,164,988, in view of Van Oorschot et al US Patent 5,699,431.

6. As per claims 1, 12, 16, 25, and 29, Matyas discloses a computer network security system having an enforceable security policy (see for example; abstract) comprising: means, operatively coupled to means for providing, for associating a digital signature of a central security policy rule data distribution source (see for example; certification center, col 11 ln 13-25) to the security policy rule data and means for storing the digital signature (see for example col 14 ln 54-col 15 ln 15); and network node means, operatively coupled to the storage means, for periodically obtaining the signature and the variable policy rule data from the means for scoring (see for example, col 16 ln 10-25), and for analyzing policy rule data to facilitate unilateral security policy enforcement at a network node level (see for example; col 9 ln 15-51).

As for obtaining the signature and the policy rule data not from a forwarded signed message, Matyas further discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 - col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system.

Matyas does not explicitly teach a variable security policy. However within the same field of endeavor Van Oorschot teaches an efficient management of CRL and update information (see abstract) including storing and managing variable security policy rule data at a network node [column 4, lines 4-44 and abstract], which provides the advantage of efficient and unilateral updating of certificates or signatures. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the method of managing, storing and providing variable security policy rule data as taught by Van Oorschot within the security system of Matyas in order to gain the advantage of efficient and unilateral updating of certificates or signatures.

7. As per claims 2, 13, 17, 26, 35, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses means for providing a user interface means for facilitating selection of security policy rule data (see for example, col 12 ln 56-col 13 ln 14).

8. As per claims 3, 14, 27, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses means for providing the security policy rule data from a data file (see for example; fig 2 and col 13 ln 1-14).

9. As per claims 4, 15, 18, 28, and 36, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses selection of policy rule data on a per network node basis for central policy definition for the at least one network node (see for example, col 11 ln 5-13).

10. As per claims 5, 19, and 37, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses associating a digital signature to the policy rule data to create a policy certificate (see for example, col 11 ln 26-col 12 ln 9).

11. As per claims 6 and 20, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses means for storing policy rule data (see for example, col 5 ln 5-25); and means, operatively coupled to the means for storing, for using policy rule analysis data to decode the policy data to facilitate security policy enforcement at a network node level (see for example, col 11 ln 26-50).

12. As per claims 7, 32, and 38, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Van Orschot further discloses variable policy rule data includes at least security policy identification data and policy rule setting data [column 4, lines 4-44 and abstract]

13. As per claims 8 and 21, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Van Orschot further discloses variable policy rule data includes policy rule priority ration data [column 4, lines 4-44 and abstract].

14. As per claim 9, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). As for policy rule data includes policy rule data on a per application basis for a plurality of software applications supported by at least one network node, Matyas further discloses differing policy rules for several applications (clients) supported by the system (see for

example, col 11 ln 1-13), therefore the policy rule data includes policy rule data on a per application basis for a plurality of applications (clients) supported by at least one network node.

15. As per claims 10 and 23, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses storing a policy certificate for distribution to the network node under control of the network node (see for example; col 6 ln 58-67).

16. As per claim 11, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses stores a policy certificate for distribution to the network nodes under control of the means for associating (see for example; col 9 ln 15-51).

17. As per claims 22 and 31, Matyas-Van Orschot disclose the claim limitations above (see for example claim 16). Matyas further discloses policy rule data includes differing policy rule data for a plurality of software applications supported by at least one network node (see for example; col 11 ln 1-13).

18. As per claim 24, Matyas-Van Orschot disclose the claim limitations above (see for example claim 1). Matyas further discloses stores a policy certificate for distribution to the network nodes under control of a network server (see for example; fig 1 and col 10 ln 41-61). Network servers are well known in the art to provide services such as distribution of data to network nodes. One of ordinary skill in the art at the time of the applicant's invention would have recognized the certification authority to be such a network server for controlling distribution of policy certificates in such a system.

19. As per claim 30, Matyas-Van Orschot disclose the claim limitations above (see for example claim 29). Matyas further discloses means for storing policy rule data (see for example, col 5 ln 5-25), and wherein the means for analyzing the policy rule data includes means for storing policy rule analysis data for evaluating the policy rule data (see for example; col 11 ln 42-50) and means, operatively coupled to the means for storing and the means for storing policy rule analysis data, for using the policy rule analysis data to decode the policy rule data to facilitate security policy enforcement at a network level (see for example, col 11 ln 26-50).

20. As per claim 33, Matyas-Van Orschot disclose the claim limitations above (see for example claim 29). Matyas further discloses the policy rule data includes policy rule prioritization data (see for example, col 6 ln 44-53; trust realm is prioritized through which realm should be selected when more than one common realm exists) and wherein the means for periodically obtaining obtains a digital signature corresponding to the policy rule data (see for example, col 11 ln 26-col 12 ln 9).

21. As per claim 34, Matyas discloses means for storing programming instructions (see for example col 12 ln 10-20) that facilitate storing security policy rule data for use by a network node (see for example col 14 ln 54col 15 ln 15); and means for storing programming instructions (see for example col 12 ln 10-20) that facilitate providing the security policy rule data for distributions to at least one network node (see for example, col 16 ln 10-25) to facilitate unilateral security policy enforcement at a network level (see for example; col 9 ln 15-51).

As for obtaining policy rule data not from a forwarded signed message, Matyas further discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made



Art Unit: 2135

unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 - col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system

Matyas does not explicitly teach a variable security policy. However within the same field of endeavor Van Oorschot teaches an efficient management of CRL and update information (see abstract) including storing and managing variable security policy rule data at a network node [column 4, lines 4-44 and abstract], which provides the advantage of efficient and unilateral updating of certificates or signatures. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the method of managing, storing and providing variable security policy rule data as taught by Van Oorschot within the security system of Matyas in order to gain the advantage of efficient and unilateral updating of certificates or signatures.

22. As per claim 39, Matyas-Van Oorschot disclose the claim limitations above (see for example claim 1). Matyas farther discloses central security policy rule data distribution source is a certification authority (see for example; certification authority, col 10 ln 62-65).

23. As per claim 40, Matyas-Van Oorschot disclose the claim limitations above (see for example claim 1). Van Oorschot further discloses variable policy rule data includes policy rule data on a per node basis [column 4, lines 4-44 and abstract].

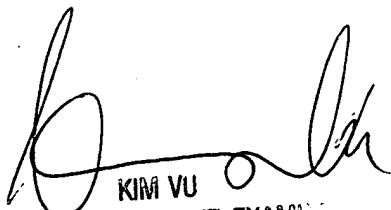
### ***Conclusion***

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada  
January 22, 2005

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 21